楕円曲線上のスカラー倍計算の効率化　：　ヤコビアン座標系上での直接計算法の提案 (計算機科学基礎理論の新展開)

AUTHOR(S):

安達, 大亮; 平田, 富夫

数理解析研究所講究録 1375 巻 2004 年 195-200

楕円曲線上のスカラー倍計算の効率化

— ヤコビアン座標系上での直接計算法の提案 —

安達 大亮 (Daisuke ADACHI)　　平田 富夫 (Tomio HIRATA)

名古屋大学大学院工学研究科　Graduate School of Engeneering, Nagoya University

〒 464-8603 名古屋市千種区不老町　464-8603 Furou, Chikusa-ku, Nagoya-Shi, Japan

Tel :052-789-3440,　Fax :052-789-3089

E-mail: adachi@hirata.nuee.nagoya-u.ac.jp, hirata@is.nagoya-u.ac.jp

概 要

楕円曲線上のスカラー倍計算は，基本演算である加算 $P \oplus Q$ や 2 倍算 $2P$ を用いて行なわれる．ここで，P, Q は楕円曲線上の点である．スカラー倍点 eP を計算する基本的な方法として窓計算法がある．窓計算法では $2^k P \oplus Q$ という形の計算を反復する．本論文では重み付き射影座標系に注目し，$2^k P \oplus Q$ を効率良く計算する方法を提案する．具体的には，$2^k P$ 直接計算法と $2P \oplus Q$ 直接計算法をそれぞれ提案し，両者を組み合わせることで計算の効率化を図っている．

1 まえがき

楕円曲線は代数曲線の一種である．この曲線上の点集合と，点の間に定義できる演算 $\oplus$ は可換群を成す．この群は有限体上の乗法群と同型である．したがって，楕円曲線上の可換群での eR の計算は，乗法群での x^e の計算と同じ方法で行うことができる．ここで，e は自然数であり，R は楕円曲線上の点である．スカラー倍計算とは，このような eR の計算を指す．

スカラー倍計算の効率化は，楕円曲線に基づく暗号システムを効率良く動作させるために重要である．このような用途では，e が数百ビット程度の極めて大きな数である．そのため，窓計算法と呼ばれる $\mathcal{O}(\log_2 e)$ 時間の計算法が用いられる．窓計算法における計算の大半は，$2^k P \oplus Q$ という形の計算の繰り返しである．ここで，P, Q は無限遠点を除く楕円曲線上の点であり，k は自然数である．

本論文では，GF(p) 上で定義された Weierstrass 型楕円曲線に注目し，その上で行われる窓計算法の効率化を提案する．具体的には，重み付き射影座標系（weighted projective 座標系，Jacobian 座標系ともいう）[4] に注目し，その上で動作する $2^k P$ 直接計算法，および $2P \oplus Q$ 直接計算法を提案する．そして，これらを併用することで $2^k P \oplus Q$ の計算コストを削減する．

以下では，p を 5 以上の素数とする．このとき，GF(p) 上で定義された Weierstrass 型楕円曲線は $y^2 \equiv x^3 + ax + b \pmod{p}$ で与えられる．ここで，$a \in \mathrm{GF}(p)$ は任意の値とする．

2 記法，窓計算法

2.1 記法

$\mathcal{S}, \mathcal{M}, \mathcal{I}$ を，それぞれ GF(p) 上の平方算，乗算，逆元計算を表す記号とする．また，各記号とそれらが指し示す各演算の平均計算時間とを同一視する場合もある．本論文では，アルゴリズムの「計算コスト」をその内部で実行された $\mathcal{S}, \mathcal{M}, \mathcal{I}$ の回数で表現する[1]．$\mathcal{S}, \mathcal{M}, \mathcal{I}$ の間には $0.8\mathcal{M} \leq \mathcal{S} < \mathcal{M}$ および $\mathcal{I} \geq 10.0\mathcal{M}$ が成立するものと仮定する．このような仮定は [4, 6] においても採用されている．例えば，[6] の実験環境では，p が 160 ビットの数であるとき $\mathcal{I} = 25.0\mathcal{M}$ と報告されている．

2.2 窓計算法

一般に，窓計算法では窓の個数を少なくするために，e の表現として NAF(Non Adjacent Form) という形式の符号付二進表現を用いる．この形式では非零ビットが隣接しない．本論文では，NAF である符号付 2 進表現を使用する．この場合，窓計算法は以下のような 3 つのステップで構成される．

【e の NAF を用いた窓計算法】

[1] その他の体演算（加減算、小さな定数による乗算など）の計算時間はこれらの十分の一以下であり考慮に入れない．

入力 楕円曲線上の点 R, 自然数 e
出力 スカラー倍点 eR
Step 1. [窓 w_i, シフト幅 s_i の設定]
$e = 2^{s_0}(2^{s_1}(\cdots(2^{s_r}w_r + w_{r-1})\cdots) + w_0)$
となる w_i, s_i を求める (w_i : odd, $|w_i| \leq 2^l - 1$,
$s_0 \geq 0$, $s_i \geq 2$ $(i = 1, 2, \ldots, r)$)
Step 2. [前計算部（窓に対応する点の計算）]
$R, 3R, \ldots, (2^K + 1)R$ を計算する
Step 3. [主計算部（eR の計算）]
$eR = 2^{s_0}(2^{s_1}(\cdots(2^{s_r}w_rR \oplus w_{r-1}R)\cdots) \oplus w_0R)$
を計算する

l は窓の長さの最大値を，K は前計算する点の個数を定めるパラメータである．K については，$K+1 = (2^l - (-1)^l)/3$ とすればよいことが知られている [2]．

主計算部では，$2^kP \oplus Q$ の形の計算を r 回繰り返す．したがって，$2^kP \oplus Q$ の計算コストの削減はスカラー倍計算の効率化につながる．

3 直接計算法

例えば，2^kP は P から 2 倍算を k 回繰り返して計算できる．このとき，$2P, 4P, \ldots, 2^kP$ を順次計算する．しかし，最終的には 2^k 以外の点（中間点）の座標は必要ない．そこで，2^kP 直接計算法では P から 2^kP の座標だけを直接計算する．同様に，$2P \oplus Q$ 直接計算法では $2P \oplus Q$ の座標だけを直接計算する．

アフィン座標系 [4] において，直接計算法は逆元計算の回数削減に効果がある [1, 6]．また，重み付き射影座標系のような他の座標系においても，計算コストの削減に効果がある [3, 5, 6]．GF(p) 上の Weierstrass 型楕円曲線の場合，上に挙げた 2 種類の方法が提案されている．

3.1 2^kP 直接計算法

2^kP 直接計算法は，$2^kP \oplus Q$ という形の計算の中で 2^kP の計算に用いられる．代表的な計算法として，酒井-櫻井の方法 [6] がある．これは任意の自然数 k に対して有効な方法である．アフィン座標系での計算法を以下に示す．各ステップの計算コストを括弧内に示す．

【酒井-櫻井の方法（アフィン座標系）】
入力 $P_1 = (x_1, y_1)$
出力 $P_{2^k} = 2^kP_1 = (x_{2^k}, y_{2^k})$
Step 1. [A_1, B_1, C_1 の計算] $(\mathcal{S})$
$A_1 = x_1, \quad B_1 = 3{x_1}^2 + a, \quad C_1 = -y_1$
Step 2. [A_i, B_i, C_i $(i = 2, 3, \ldots, k)$ の計算]
$(4(k-1)\mathcal{S} + 3(k-1)\mathcal{M})$
$A_i = B_{i-1}^2 - 8A_{i-1}C_{i-1}^2$
$B_i = 3A_i^2 + 16^{i-1}a(\prod_{j=1}^{i-1} C_j)^4$
$C_i = -8C_{i-1}^4 - B_{i-1}(A_i - 4A_{i-1}C_{i-1}^2)$
Step 3. [D_k の計算] $(2\mathcal{S} + \mathcal{M})$
$D_k = 12A_kC_k^2 - B_k^4$
Step 4. [x_{2^k}, y_{2^k} の計算] $(2\mathcal{S} + (k+3)\mathcal{M} + \mathcal{I})$
$x_{2^k} = \frac{B_k^2 - 8A_kC_k^2}{(2^k\prod_{j=1}^{k} C_j)^2}$
$y_{2^k} = \frac{8C_k^4 - B_kD_k}{(2^k\prod_{j=1}^{k} C_j)^3}$

この計算コストは，$(4k+1)\mathcal{S} + (4k+1)\mathcal{M} + \mathcal{I}$ である．一方，2 倍算を k 回繰り返したときの計算コストは，$2k\mathcal{S} + 2k\mathcal{M} + k\mathcal{I}$ である．したがって，平方算と乗算がそれぞれ $2k+1$ 回増加する代わりに，逆元計算の回数は $k-1$ 回減少している．その結果，全体の計算コストは減少する．

中間点 $2^{i-1}P_1$ の座標計算には逆元計算が必要である．この方法では，$2^{i-1}P_1$ の座標を計算せず，代わりにこれを A_i, B_i, C_i に分割した形で保持する．この A_i, B_i, C_i から $A_{i+1}, B_{i+1}, C_{i+1}$ を計算することで，2^kP_1 の座標を計算するときの 1 回だけに逆元計算を削減している．

[6] では，アフィン座標系での方法とともに，重み付き射影座標系での 2^kP 直接計算法も提案されている．これは，上の方法を重み付き射影座標系のために拡張したものであり，Step 2. と Step 3. は同じである．しかし，以下の点が異なる．

(1) Step 1. の前に，$P_1 = (X_1, Y_1, Z_1)$ を正規化[2]して $(X_1', Y_1', 1)$ を計算 $(\mathcal{S} + 3\mathcal{M} + \mathcal{I})$
(2) Step 1. では，上記の X_1', Y_1' を x_1, y_1 の代わりに使用

[2] $(X, Y, Z) = (X', Y', 1)$ を充たす点を計算する処理．このとき，$X' = X/Z^2$, $Y' = Y/Z^3$ が成り立つ．この式より，正規化では逆元計算が必要である．

(3) Step 4. では，$2^kP_1=(X_{2^k}, Y_{2^k}, Z_{2^k})$ を以下のように計算 $(\mathcal{S}+k\mathcal{M})$

$$X_{2^k}=B_k^2-8A_kC_k^2$$
$$Y_{2^k}=8C_k^4-B_kD_k$$
$$Z_{2^k}=2^k\prod_{j=1}^{k}C_j$$

この計算コストは，$Z_1=1$ の場合 $4k\mathcal{S}+(4k-2)\mathcal{M}$ である．また，$Z_1\neq 1$ の場合は $(4k+1)\mathcal{S}+(4k+1)\mathcal{M}+\mathcal{I}$ である．一方，2倍算を k 回繰り返したときの計算コストは，$6k\mathcal{S}+4k\mathcal{M}$ である．したがって，$Z_1=1$ の場合は計算コストが $2k\mathcal{S}+2\mathcal{M}$ 減少する．しかし，$Z_1\neq 1$ の場合は $\mathcal{I}$, k が $\mathcal{I}<(2k-1)\mathcal{S}-\mathcal{M}$ を満たすときに限り減少する．

この他にも 2^kP 直接計算法が提案されている [3, 5]．しかし，これらは $k=2$ の場合だけで有効である．

3.2 $2P\oplus Q$ 直接計算法

$2P\oplus Q$ 直接計算法は，$2^kP\oplus Q$ という形の計算の中で，$2^{k-1}P$ から $2(2^{k-1}P)\oplus Q$ を計算する際に用いられる．このような計算法として，Eisenträger-Lauter-Montgomery の方法 [1] がある．これは，アフィン座標系用の計算法である．

アフィン座標系では加算よりも2倍算の計算コストが大きいので，$2P\oplus Q$ を $(P\oplus Q)\oplus P$ という形で計算する．$P(x_1, y_1)$, $Q(x_2, y_2)$ が与えられると，まず $\lambda=(y_2-y_1)/(x_2-x_1)$ を計算した上で $P\oplus Q=P'(x_{P'}, y_{P'})$ を計算する．次に，P 及び P' から $\lambda'=(y_{P'}-y_1)/(x_{P'}-x_1)$ を計算し，これを用いて $2P\oplus Q$ を計算する．λ' の計算コストは $\mathcal{M}+\mathcal{I}$ である．ここで，$y_{P'}=\lambda(x_1-x_{P'})-y_1$ を代入すると，λ' は以下の計算式になる．

$$\lambda'=-\lambda-\frac{2y_1}{x_{P'}-x_1}$$

この式でも，λ' の計算コストは $\mathcal{M}+\mathcal{I}$ であり，かつ $y_{P'}$ が含まれていない．したがって，$2P\oplus Q$ の計算の際に $y_{P'}$ の計算（計算コスト $\mathcal{M}$）を省略できる．これが，Eisenträger-Lauter-Montgomery の方法である．$2P\oplus Q$ の計算コストは，$P\neq Q$ の場合 $2\mathcal{S}+3\mathcal{M}+2\mathcal{I}$ であり，$P=Q$ の場合は $3\mathcal{S}+3\mathcal{M}+2\mathcal{I}$ である．

4 提案する直接計算法

この章では重み付き射影座標系に注目する．

窓計算法では，$2^kP\oplus Q$ という形の計算における P は点 w_rR であるか，一つ前に行われた $2^kP\oplus Q$ の計算の結果である．したがって，その Z 座標が1である可能性は極めて小さい．従来の酒井-櫻井の 2^kP 直接計算法では，入力点 P_1 の Z 座標が1ではないときに P_1 を正規化する（3.1節）．したがって，これを窓計算法の中で用いると，正規化に含まれる逆元計算が多数回繰り返される．そこで，本論文では，正規化が不要なように改良した 2^kP 直接計算法を提案する．

一方，この座標系での $2P\oplus Q$ 直接計算法は現在提案されていない．本論文では，この座標系での $2P\oplus Q$ 直接計算法を提案する．また，上の 2^kP 直接計算法と組み合わせて $2^kP\oplus Q$ の効率の良い計算方法を実現する．

4.1 正規化なしの 2^kP 直接計算法

従来の方法を改良した 2^kP の直接計算法を示す．

【Algorithm 1: 正規化なしの 2^kP 直接計算法】

入力 $P_1=(X_1, Y_1, Z_1)$

出力 $P_{2^k}=2^kP_1=(X_{2^k}, Y_{2^k}, Z_{2^k})$

Step 1 $[A_1, B_1, C_1$ **の計算**$]$ $(3\mathcal{S}+\mathcal{M})$

$$A_1=X_1,\quad B_1=3X_1^2+aZ_1^4$$
$$C_1=-Y_1$$

Step 2 $[A_i, B_i, C_i\ (i=2, 3, \ldots, k)$ **の計算**$]$ $(4(k-1)\mathcal{S}+3(k-1)\mathcal{M})$

$$A_i=B_{i-1}^2-8A_{i-1}C_{i-1}^2$$
$$B_i=3A_i^2+16^{i-1}a(Z_1\prod_{j=1}^{i-1}C_j)^4$$
$$C_i=-8C_{i-1}^4-B_{i-1}(A_i-4A_{i-1}C_{i-1}^2)$$

Step 3 $[D_k$ **の計算**$]$ $(2\mathcal{S}+\mathcal{M})$

$$D_k=12A_kC_k^2-B_k^2$$

Step 4 $[X_{2^k}, Y_{2^k}, Z_{2^k}$ **の計算**$]$ $(\mathcal{S}+(k+1)\mathcal{M})$

$$X_{2^k}=B_k^2-8A_kC_k^2$$
$$Y_{2^k}=8C_k^4-B_kD_k$$
$$Z_{2^k}=2^kZ_1\prod_{j=1}^{k}C_j$$

$Z_1\neq 1$ の場合，計算コストは $(4k+2)\mathcal{S}+4k\mathcal{M}$ である．酒井-櫻井の方法と比較すると，$\mathcal{I}+\mathcal{M}-\mathcal{S}$ 小さくなる．$Z_1=1$ の場合は，改良版と従来の方

法は同一になる.

この改良版では，正規化を行わない代わりに，B_1 と Z_{2^k} の計算コストが増える．B_1 の計算では $2\mathcal{S}+\mathcal{M}$ 増え，Z_{2^k} の計算では $\mathcal{M}$ 増えるので，全体として計算コストは $2\mathcal{S}+2\mathcal{M}$ 増える．しかし，これは正規化のコスト $\mathcal{S}+3\mathcal{M}+\mathcal{I}$ よりも小さいので，全体の計算コストは従来の方法よりも小さくなる．

4.2 提案する $2P \oplus Q$ 直接計算法

提案する $2P \oplus Q$ 直接計算法を与える．$P \neq Q$ の場合，$2P \oplus Q$ を以下のように計算する．

【Algorithm 2 : $2P+Q$ 直接計算法 ($P \neq Q$)】
入力 $P=(X_1, Y_1, Z_1), Q=(X_2, Y_2, Z_2)$
出力 $2P \oplus Q=(X_4, Y_4, Z_4)$
Step 1 U_1, S_1, H_1, r_1 の計算 $(2\mathcal{S}+6\mathcal{M})$
$U_1=X_1Z_2^2,\ S_1=Y_1Z_2^3$
$H_1=X_2Z_1^2-U_1,\ r_1=Y_2Z_1^3-S_1$
Step 2 U_2, S_2, H_2, r_2 の計算 $(2\mathcal{S}+4\mathcal{M})$
$U_2=U_1H_1^2,\ S_2=S_1H_1^3$
$H_2=-H_1^3-3U_2+r_1^2,\ r_2=-r_1H_2-2S_2$
Step 3 X_4, Y_4, Z_4 の計算 $(2\mathcal{S}+7\mathcal{M})$
$X_4=-H_2^3-2U_2H_2^2+r_2^2$
$Y_4=-S_2H_2^3+r_2(U_2H_2^2-X_4)$
$Z_4=Z_1Z_2H_1H_2$

計算コストは $6\mathcal{S}+17\mathcal{M}$ である．一方，加算と2倍算を1回ずつ用いたときの計算コストは，$10\mathcal{S}+16\mathcal{M}$ である [4]．したがって，計算コストは $4\mathcal{S}-\mathcal{M}$ だけ小さい．

$2P \oplus Q$ を $(P \oplus Q) \oplus P$ という2回の加算として考える．この座標系では，パラメータ U_1, S_1, H_1, r_1 を計算した上で $P'=P \oplus Q$ を計算する [4]．$P' \oplus P$ を計算するときも同様である．この時の計算コストは $8\mathcal{S}+24\mathcal{M}$ である．これに対し，提案法では U_1, S_1, H_1, r_1 から2回目の加算のパラメータ U_2, S_2, H_2, r_2 を直接計算し，P' の座標計算を省略している[3]．削減された $2\mathcal{S}+7\mathcal{M}$ の計算コストのうち，大半が P' の座標を計算するコストである．

$P=Q$ の場合も同様にして $3P$ を直接計算可能であるが，本論文では省略する．

[3] $Z_{P'}$ を P' の Z 座標とする．すると $U_2=X_1Z_{P'}^2,\ Z_{P'}=Z_1Z_2H_1$ から，$U_2=U_1H_1^2Z_1^2$ が得られる．Z_1^2 については後で消去される．S_2, H_2, r_2 についても同様である．

4.3 $2^kP \oplus Q$ の計算方法

ここでは，$2^kP \oplus Q$ を計算する方法を二つ提案する．一つは，P から 2^kP を Algorithm 1 で直接計算して，Q を加える方法である．これを提案法 (1) とする．もう一つは，P から $2^{k-1}P$ を Algorithm 1 で直接計算して，更に $2(2^{k-1}P) \oplus Q$ を Algorithm 2 で直接計算する方法である[4]．これを提案法 (2) とする．

4.4 従来法との比較

重み付き射影座標系では2倍算の計算コストが加算よりも小さい．したがって，$2^kP \oplus Q$ の計算方法として，P から2倍算の繰り返しで 2^kP を計算して，Q を加える方法が考えられる．これを従来法 (1) とする．このとき，$2^kP \oplus Q$ の計算コストは以下のようになる．

従来法 (1) 2倍算と加算を使用 $((2^kP) \oplus Q)$
計算コスト：$(6k+4)\mathcal{S}+(4k+12)\mathcal{M}$
提案法 (1) Algorithm 1 と加算を使用 $((2^kP) \oplus Q)$
計算コスト：$(4k+6)\mathcal{S}+(4k+12)\mathcal{M}$
提案法 (2) Algorithm 1 と Algorithm 2 を使用
$(2(2^{k-1}P) \oplus Q)$
計算コスト：$(4k+4)\mathcal{S}+(4k+13)\mathcal{M}$

計算コストを比較すると，提案法 (2) は従来法 (1) よりも $2k\mathcal{S}-\mathcal{M}$ 小さく，提案法 (1) よりも $2\mathcal{S}-\mathcal{M}$ 小さい．$0.8\mathcal{M} \leq \mathcal{S}$ より，提案法 (2) における $2^kP \oplus Q$ の計算コストは従来の方法よりも減少する．以下では，提案法 (2) を単に提案法と呼ぶ．

5 他の座標系における計算コスト

スカラー倍計算では，重み付き射影座標系の他にもアフィン座標系 [4] や修正ヤコビアン座標系 (modified Jacobian 座標系) [4] が使用される．この章では，提案法における $2^kP \oplus Q$ の計算コストをこれらの座標系を用いた従来の方法と比較する．

[4] $k \geq 2$ であるため，$2P \oplus Q$ 直接計算法を用いるときには必ず $P \neq Q$ である．

表 1: $2^kP \oplus Q$ の計算コスト（$k = 5$）

計算法	計算コスト	$\mathcal{I} = 10.0\mathcal{M}$	コストの差
提案法	$24\mathcal{S} + 33\mathcal{M}$	$24\mathcal{S} + 33\mathcal{M}$	—
従来法 (2)	$10\mathcal{S} + 12\mathcal{M} + 6\mathcal{I}$	$10\mathcal{S} + 72\mathcal{M}$	$39\mathcal{M} - 14\mathcal{S}$
従来法 (3)	$22\mathcal{S} + 23\mathcal{M} + 2\mathcal{I}$	$22\mathcal{S} + 43\mathcal{M}$	$10\mathcal{M} - 2\mathcal{S}$
従来法 (4)	$19\mathcal{S} + 20\mathcal{M} + 3\mathcal{I}$	$19\mathcal{S} + 50\mathcal{M}$	$17\mathcal{M} - 5\mathcal{S}$

5.1 アフィン座標系との比較

アフィン座標系では2倍算の計算コストが加算よりも大きい．したがって，2倍算と加算を用いる方法では，まず P から2倍算を繰り返して $2^{k-1}P$ を計算して，それから $(2^{k-1}P \oplus Q) \oplus 2^{k-1}P$ を計算する．これを従来法 (2) とする．一方，直接計算法として酒井-櫻井の方法及び Eisentrager-Lauter-Montgomery の方法を用いることを考える．提案法 (1) と同様の計算をする方法を従来法 (3) とする．また，提案法 (2) と同様の計算をする方法を従来法 (4) とする．このとき，$2^kP \oplus Q$ の計算コストは以下のようになる．

従来法 (2) 2倍算と加算を使用
$((2^{k-1}P \oplus Q) \oplus 2^{k-1}P)$
計算コスト：$2k\mathcal{S} + (2k+2)\mathcal{M} + (k+1)\mathcal{I}$

従来法 (3) 酒井-櫻井の方法と加算を使用
$((2^kP) \oplus Q)$
計算コスト：$(4k+2)\mathcal{S} + (4k+3)\mathcal{M} + 2\mathcal{I}$

従来法 (4) 酒井-櫻井の方法と Eisenträger らの方法を使用
$(2(2^{k-1}P) \oplus Q)$
計算コスト：$(4k-1)\mathcal{S} + 4k\mathcal{M} + 3\mathcal{I}$

この座標系での計算コストは，k の値と $\mathcal{I}$ のコストによって大小関係が変化する．そのため，各計算法の優劣を単純に比較できない．そこで，条件を $k = 5, \mathcal{I} = 10.0\mathcal{M}$ に固定して，提案法の計算コストを従来法 (2) から従来法 (4) と比較した（表1）．コストの差の欄は，各計算方法の計算コストから提案法の計算コストを引いたものである．すると，$\mathcal{S} < \mathcal{M}$ であるから，それらの値は何れの従来法についても正の値となる．したがって，提案法の計算コストは何れの従来法に対しても小さくなる．$\mathcal{I} \geq 8.0\mathcal{M}$ である限り，その他の k の値についても同様である．

5.2 修正ヤコビアン座標系との比較

次に，修正ヤコビアン座標系で，$2^kP \oplus Q$ の計算コストを考える．重み付き射影座標系を改良した結果，加算の計算コストは $6\mathcal{S} + 13\mathcal{M}$ と大きくなるが，2倍算の計算コストは $4\mathcal{S} + 4\mathcal{M}$ と小さくなる．

この座標系では2倍算の計算コストが加算よりも小さい．また，現在までに，この座標系での直接計算法は提案されていない．したがって，k 回の2倍算で 2^kP を計算して Q を加える方法だけを考える．これを従来法 (5) とする．その計算コストは $k(4\mathcal{S}+4\mathcal{M})+(6\mathcal{S}+13\mathcal{M}) = (4k+6)\mathcal{S}+(4k+13)\mathcal{M}$ である．したがって，提案法の方が，計算コストが $2\mathcal{S}$ 小さくなる．

以上より，提案法は他の座標系でのどの従来法よりも計算コストが小さくなる．

6 まとめ

本論文では，重み付き射影座標系に注目し，酒井-櫻井の方法を改良した 2^kP 直接計算法を与えた．また，従来の加算と2倍算による方法よりも効率が良い $2P \oplus Q$ の直接計算法を提案した．そして，この両者を併用した $2^kP \oplus Q$ の計算法を提案し，従来の方法よりも窓計算法の計算コストが削減されることを理論的に示した．

参考文献

[1] K. Eisenträger, K. Lauter, P.L. Montgomery, "An efficient procedure to double and add points on an elliptic curve", IACR Cryptology ePrint Archive, 2002. available at: http://eprint.iacr.org/2002/112.ps.gz

[2] N. Kunihiro, and H. Yamamoto, "Window and extended window methods for addition chain and addition-subtraction chain," IEICE Trans. Fundametals, vol.E81-A, no.1, pp.72–81, 1998.

[3] A. Miyaji, T. Ono and H. Cohen, "Efficient elliptic curve exponentiation (I)", IEICE Technical Report, ISEC97-16, 1997.

[4] H. Cohen, A. Miyaji and T. Ono "Efficient elliptic curve exponentiation using mixed coordinates", Advances in Cryptology–ASIACRYPT'98, LNCS, vol.1514, pp.51–65, Springer-Verlag, 1998.

[5] V. Müller, "Efficient algorithms for multiplication on elliptic curves", Proc. GI-Arbeitskonferenz Chipkarten 1998, TU München, 1998.

[6] Y. Sakai, K. Sakurai, "Efficient scalar multiplications on elliptic curves with direct computations of several doublings", IEICE Trans. Fundamentals, Vol.E84-A, No.1, Jan, 2001.

[7] J.H. Silverman, The Arithmetic of Elliptic Curves, GTM106, Springer-Verlag, 1986.